Chapter

A Geometrical Realisation of Quasi-Cyclic Codes

Cristina Martinez Ramirez and Alberto Besana

Abstract

We study and enumerate cyclic codes which include generalised Reed-Solomon codes as function field codes. This geometrical approach allows to construct longer codes and to get more information on the parameters defining the codes. We provide a closed formula in terms of Stirling numbers for the number of irreducible polynomials and we relate it with other formulas existing in the literature. Further, we study quasi-cyclic codes as orbit codes in the Grassmannian parameterizing constant dimension codes. In addition, we review Horn's algorithm and apply it to construct classical codes by their defining ideals.

Keywords: cyclic code, partition, Grassmannian

1. Introduction

Function fields are used ubiquitously in algebraic coding theory for their flexibility in constructions and have produced excellent linear codes. Suitable families of function fields, for example good towers of function fields, have been used to construct families of codes with parameters bound better than the asymptotic bound.

Let q a power of a prime number p. It is well known, that there exists exactly one finite field with q elements which is isomorphic to the splitting field of the polynomial $x^q - x$ over the prime field $\mathbb{F}_p$. Any other field F of characteristic p contains a copy of $\mathbb{F}_p$. We denote respectively by $\mathbb{A}^n(\mathbb{F}_q)$ and $\mathbb{P}^n(\mathbb{F}_q)$ the affine space and the projective space over $\mathbb{F}_q$. Let $\mathbb{F}_q[x_1, x_2, \dots, x_n]$ be the algebra of polynomials in n variables over $\mathbb{F}_q$.

The encoding of an information word into a k-dimensional subspace is usually known as coding for errors and erasures in random network coding [1]. Namely, let V be an $N-$dimensional vector space over $\mathbb{F}_q$, a code for an operator channel with ambient space V is simply a non-empty collection of subspaces of V. The collection of subspaces is a code for error correcting errors that happen to send data through an operator channel. The matrix coding the information is parameterised by random variables $a_1, a_2, \dots, a_n$ which constitute the letters of an alphabet. Here the operator channel is an abstraction of the operator encountered in random linear network coding, when neither transmitter nor receiver has knowledge of the channel transfer characteristics. The input and output alphabet for an operator channel is the projective geometry. A good code is capable of correcting error and erasures at the output of the operator channel. Thus in order to construct good codes one need to choose a metric consistent with channel errors and search of a set of vectors with given metric properties as a correcting code. The codes considered here are codes for channels whose errors are consistent with the weighted Hamming metric (WHM).

Let $\mathcal{C}$ be a non-singular, projective, irreducible curve defined over $\mathbb{F}_q$, as the vanishing locus of a polynomial $F \in \mathbb{F}_q[x_0, x_1, x_2]$. We define the number $N(q)$ of $\mathbb{F}_q-$rational points on the curve to be

$$N(q) = \ |\{(x_0, x_1, x_2) \in \mathbb{P}^2(\mathbb{F}_q) | F(x_0, x_1, x_2) = 0\}|.$$

It is a polynomial in q with integer coefficients, whenever q is a prime power.

The number of points $\overline{\mathcal{C}}(\mathbb{F}_{q^r})$ on $\mathcal{C}$ over the extensions $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$ is encoded in an exponential generating series, called the zeta function of $\overline{\mathcal{C}}$:

$$Z(\mathcal{C}, t) = exp\left(\sum_{r=1}^{\infty} \#\overline{\mathcal{C}}(\mathbb{F}_{q^r}) \frac{t^r}{r}\right).$$

Garcia and Stichtenoth analysed the asymptotic behaviour of the number of rational places and the genus in towers of function fields, [2]. From Garcia-Stichtenoth's second tower one obtains codes over any field $\mathbb{F}_q$ where q is an even power of a prime [3].

One of the main problems in coding theory is to obtain non-trivial lower bounds of the number $N(F_i)$ of rational places of towers of function fields $\{F_i/\mathbb{F}_q\}_{i=1}^{\infty}$ such that $F_i \subsetneq F_{i+1}$. Suitable families of function fields, for example good towers of function fields, have been used to construct families of codes that beat the Gilbert-Varshamov bound. This paper aims to explore this link for the study and construction of quasi-cyclic codes. For example good codes are obtained for curves of genus 0, they are in fact extended generalised Reed-Solomon codes.

Notation. Let $\mathbb{F}_q$ denote the Galois field of q elements and let $(\mathbb{F}_q)^n$ denote the vector spaces of all ordered n-tuples over $\mathbb{F}_q$. The Hamming weight of a vector x, denoted by $wt(x)$ is then number of non-zero entries in x. A linear code C of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of $(\mathbb{F}_q)^n$. Such a code is called $[n, k, d]_q$ code if its minimum Hamming distance is d. For d a positive integer, $\alpha = (\alpha_1, \dots, \alpha_m)$ is a partition of d into m parts if the α_i are positive and decreasing.

2. Algebraic geometric codes

Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of a prime. We consider as an alphabet a set $\mathcal{P} = \{P_1, \dots, P_N\}$ of $N - \mathbb{F}_q$ rational points lying on a smooth projective curve $\mathcal{C}$ of genus g and degree d defined over the field $\mathbb{F}_q$. If D is a divisor on the curve $\mathcal{C}$, $\mathcal{L}(D)$ is the linear series attached to this divisor with coefficients in the field.

Definition 2.1. *Algebraic Geometric Codes (AGC) are constructed by evaluation of the global sections of a line bundle or a vector bundle on the curve $\mathcal{C}$ over N $(N > g)$ distinct rational places $P_1, \dots, P_N$. Namely, let $F|\mathbb{F}_q$ be the function field of the curve, $\mathcal{D}$ the divisor $P_1 + \cdots + P_N$ and G a divisor of $F|\mathbb{F}_q$ of degree $s \leq N$ such that* $\text{Supp} \ \ G \cap \text{Supp} \ \ D = \text{ø}$. *Then the geometric Goppa code associated with the divisors D and G is defined by*

$$\mathbf{C}(D, G) = \{(x(P_1), \dots, x(P_n)) | x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_{q^n}.$$

Recall that $\mathbb{F}_{q^n}|\mathbb{F}_q$ is a cyclic Galois extension and it is finitely generated by unique element $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$. α is a primitive element and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of the field extension $\mathbb{F}_q \hookrightarrow \mathbb{F}_q(\alpha)$, that is, $\mathbb{F}_{q^n} \cong (\mathbb{F}_q)^n$.

In the sequel, an $[n,k]_q$-code C is a k-dimensional subspace of $(\mathbb{F}_q)^n$.

2.1 Generalised Reed-Solomon codes as cyclic codes

Another important family of Goppa codes is obtained considering the normal rational curve (NRC) $\mathcal{C}^n$ defined over $\mathbb{F}_q$:

$$\mathcal{C}^n := \{\mathbb{F}_q(1, \alpha, \ldots, \alpha^n) : \alpha \in \mathbb{F}_q \cup \{\infty\}\}.$$

Assuming that $(n,p) = 1$ are coprime, the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forms a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where p is the characteristic of the field. Thus points in the NRC are in correspondence with $\mathbb{F}_q-$linear combinations of the base vectors up to collineation. The Goppa codes of dimension n defined over $\mathcal{C}^n$ are constructed by evaluating non-zero polynomials of degree less than n over a sequence $\alpha_1, \ldots, \alpha_n$ of n distinct elements in $\mathbb{F}_q$, if $k \leq n$, then the map

$$\epsilon : \mathbb{F}_q[x] \to \mathbb{F}_q^n, \quad f \mapsto (f(\alpha_1, \ldots, \alpha_n)) \tag{1}$$

is injective, since the existence of a non-zero polynomial of degree less than k vanishing on all α_i implies $n < k$ by the fundamental theorem of algebra (a non-zero polynomial of degree r with coefficients in a field can have at most r roots). These are just Reed-Solomon codes of parameters $[n, k, d]$ over a finite field $\mathbb{F}_q$, with parity check polynomial $h(x) = \prod_{i=1}^{q}(x - \alpha^i)$, where α is a primitive root of $\mathbb{F}_q$ such that $\alpha^{k+1} = \alpha + 1$. Any codeword $(c_0, c_1, \ldots, c_{n-1})$ can be expanded into a q-ary k vector with respect to the basis $\{1, \alpha, \ldots, \alpha^{k-1}\}$. Construction of generalised Reed-Solomon codes over $\mathbb{F}_q$ only employ elements of $\mathbb{F}_q$, hence their lengths are at most $q+1$. In order to get longer codes, one can make use of elements of an extension of $\mathbb{F}_q$, for instance considering subfield subcodes of Reed-Solomon codes. In this way, one gets cyclic codes. Recall that a linear cyclic code is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by a polynomial $g(x)$ with roots in the splitting field $\mathbb{F}_q^l$ of $x^n - 1$, where $n|q^l - 1$, ([4]). We shall identify the code with the set of its codewords. A natural question then to ask is how many irreducible polynomials of degree at least 2 are there over the algebraic closure of $\mathbb{F}_q[x]$. Next theorem expresses this number in terms of Stirling numbers.

Theorem 2.2. *Assume that $(q,n) = 1$, then the number of polynomials of degree $(n \geq 2)$ decomposable into distinct linear factors over a finite field $\mathbb{F}_q$ of arbitrary characteristic a prime number p, is equal to $\sum_{k=1}^{n}(q)_k$, where $(q)_k$ is the falling factorial polynomial $q \cdot (q-1) \ldots (q-k) = \sum_{k=0}^{n} s(n,k) q^k$, where $s(n,k)$ is the Stirling number of the first kind (the number of ways to partition a set of n objects into k non-empty subsets), divided by the order of the affine transformation group of the affine line $\mathbb{A}^1 = \mathbb{P}^1 \backslash \infty$, that is $q^2 - q$.*

Proof. We need to count all the polynomials $f_n(x)$ in one variable of degree n fixed. We assume that our polynomial $f_n(x)$ decomposes into linear factors, otherwise we work over $\overline{\mathbb{F}}_q[x]$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of the finite field $\mathbb{F}_q$. Since the number of ordered sequences on q symbols is $q!$ and each root is counted with its multiplicity, it follows that the number of monic polynomials with $n-1$

different roots is $q(q-1)(q-2)\ldots(q-n+1) := (q-2)_n$. Now we observe that polynomials are invariant by the action of automorphisms of the affine line, so we must divide this number by the order of this group which is $q^2 - q$. □

Theorem 2.3. *Given a set of integers $\{0, 1, \ldots, n-1\}$ module n, there is a set J of k integers which is a set of roots, that is, there is a polynomial $h(x) = \prod_{j\in J}(x - \alpha^j)$, where α is a generator of $(\mathbb{F}_{p^m})$ for some prime number p and m is the least integer such that $n|p^m - 1$. The ideal $h(x)$ generates in $\mathbb{F}_{p^m}[x]/(x^n - 1)$ is a cyclic linear code of parameters $(n, k, n-k+1)$.*

Proof. Let m be the least integer such that n divides $p^m - 1$, then $g.c.d(m,p) = 1$. We define an equivalence relation on the set of integers $\{0, 1, \ldots, n-1\}$, by declaring two integers i and j in the range $0 \le i \le n-1$ to be conjugate module n if $p^s i \equiv j \pmod n$. This equivalence relation partition the set into cyclotomic cosets. The cyclotomic coset containing j, which we will denote by Ω_j, can be described explicitly as the set $\{j, pj, \ldots, p^{k-1}j\}$, where k is the least positive integer such that $p^k j \equiv j \pmod n$ and j is not necessarily the smallest integer in such coset. Denote by I_n the set consisting of the smallest integers in each cyclotomic coset, then I_n is a set root, that is, it is a set of k integers in arithmetic progression modulo n whose increment is relatively prime to n. Let $d = n - k + 1$, then the polynomial $\prod_{i\in I_n}(x - \alpha^i)$ defines a cyclic code of parameters (n, k, d). □

As an application of Theorem 2.2, given an integer n, we can count the number of cyclic codes of parameters $[n, k]$ for each $0 \le k \le n$ and set of roots $\alpha_1, \ldots, \alpha_k$ in the splitting field of $x^n - 1$, the corresponding polynomial $g(x) = \prod_{i=1}^{k}(x - \alpha_i)$ generates a linear cyclic code in the ring $\mathbb{F}_q[x]/(x^n - 1)$. Thus for each $0 \le k \le n$ there are exactly $(q)_k/(q^2 - q)$ cyclic codes.

In the theory of error-correcting codes to a given code $C \subset \mathbb{F}_q^n$, one assigns another important parameter, the minimum distance d which measures how good the decoding is.

Definition 2.4. *The distance between vectors $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ in the Weighted Hamming metric (WHM) is defined by a function:*

$$d_{WH}(a,b) = \sum_{i=1}^{n} w_i \overline{d(a_i, b_i)},$$

where $w_i > 0$, $d(a_i, b_i) = 1$ if $a_i \ne b_i$ and $d(a_i, b_i) = 0$ if $a_i = b_i$. The weight of a vector a in the WHM is $wt_{WH}(a) = d_{WH}(a, 0) = \sum_{i:a_i\ne 0} w_i$. The value w_i and vector $w = (w_1, w_2, \ldots, w_n)$ are called a weight of position i and a vector of weights of positions respectively.

Geometrically a binary vector $(a_1, \ldots, a_n)$ of length n gives the coordinates of a vertex of a unit cube in n dimensions.

Example 1. *Consider the Goppa code defined by the rational function $g(x) = \frac{3x^2-5x+5}{x^3-2x^2+x}$ which admits as decomposition into partial fractions the expression $G(x) := \frac{5}{x} - \frac{2}{x-1} + \frac{3}{(x-1)^2}$. The presence of a double factor $(x-1)^2$ corresponds to the existence of an eigenspace E in the vector space $\mathbb{F}_q^n$ of multiplicity 2 and thus an $\alpha-$splitting subspace where the operator α is just the linear operator $A - \lambda I$, with λ the eigenvalue associated to E and A is the generator matrix of the code. We recall that an $r-$dimensional W subspace is $\alpha-$splitting if $\alpha^i W = W$ is invariant under the action of any element α^i in the Galois group of the extension $\mathbb{F}_q \rightarrowtail \mathbb{F}_q(\alpha)$.*

2.2 Algebraic function field codes

A much greater variety of linear codes is obtained if one uses places of arbitrary degree rather than just places of degree 1. These codes are more naturally described through function field codes. A general viewpoint is that function field codes are certain finite dimensional linear subspaces of an algebraic function field over a finite field as in Goppa's construction.

In the paper [5], the authors introduce another construction where places of arbitrary degree are allowed. The method consists of choosing two divisors G_1 and G_2 of an algebraic curve over $\mathbb{F}_q$ with $G_1 \leq G_2$. Then $\mathcal{L}(G_1)$ is a subspace of the vector space $\mathcal{L}(G_2)$ over $\mathbb{F}_q$. If we choose a basis of $\mathcal{L}(G_2)$, then the coordinate vectors of the elements of $\mathcal{L}(G_1)$ form a linear code over $\mathbb{F}_q$ of length $n = \dim(\mathcal{L}(G_2))$ and dimension $k = \dim(\mathcal{L}(G_1))$. These are known as function field codes and they provide a general perspective on the construction of algebraic-geometry codes [6].

Example 2. *We consider as in* [7] *the Suzuki curve* χ *defined over* $\mathbb{F}_q$ *by the following equation* $y^q - y = x^{q_0}(x^q - x)$ *with* $q = 2q_0^2 \geq 8$ *and* $q_0 = 2^r$. *This curve has exactly* $q^2 + 1-$*rational places with a single place at infinity* P_∞ *and it is of genus* $g_S = q_0(q-1)$. *We construct a code out of the divisor* $F = mP_\infty$ *and* Q *where* $Q = P_1 + \dots + P_{q^2}$ *is the sum of the* q^2-*rational points and the parameter* m *satisfies the bound* $m > 2g - 2$ *and* g *is the genus of the curve.*

Observe that the geometric Goppa code $\mathbf{C}(F, Q)$ is an $\mathbb{F}_q$-subspace of $(\mathbb{F}_q)^{q^2}$ and its dimension k as an $\mathbb{F}_q-$vector space is the dimension of the code. Geometrically, it corresponds to a point in the Grassmannian $\mathcal{G}_{q^2,k}(\mathbb{F}_q)$. The set of codewords recognised by the code $\mathbf{C}(F, Q)$ admits the following description in terms of monomial ideals in the variables x, y, z, w:

$$\left\{x^a y^b z^c w^{d'} \,|\, a, b, c, d' \geq 0, aq + b(q + q_0) + c(q + 2q_0) + d'(q + 2q_0 + 1) \leq d\right\},$$

where $z = x^{2q_0+1}$ and $w = xy^{2q_0} - z^{2q_0}$ are elements in the function field $F_\chi := \mathbb{F}_q(x, y)$ over $\mathbb{F}_q$. Moreover, it is a generating set for the linear series $\mathcal{L}(dP_\infty)$ associated to the divisor dP_∞.

Theorem 2.5. *Cyclic codes are function field codes constructed over the curve* $\mathcal{C}_{n,m}$ *with affine equation* $y^m + x^n = 1$ *defined over a finite field* $\mathbb{F}_q$ *of* q *elements, where* q *is a power of a prime* p *and* n, m *are integer numbers greater or equal than 2.*

Proof. Let us assume n is an integer even number, thus $n = 2^k \cdot s$, with s an integer odd number. We recall that a linear cyclic code is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by a polynomial $g(x)$ with roots in the splitting field $\mathbb{F}_q^l$ of $x^n - 1$, where $n | q^l - 1$. If we consider the factorisation of the polynomial $x^n - 1$ over $\mathbb{F}_p[x]$, we get $(x^{n/2} - 1)(x^{n/2} + 1) = (x^{n/4} - 1)(x^{n/4} + 1)(x^{n/2} + 1) = \left(x^{n/2^k} - 1\right)\left(x^{n/2^k} + 1\right)\left(x^{n/2^{(k-1)}} - 1\right)\left(x^{n/2^{(k-1)}} + 1\right) \dots (x^{n/2} + 1)$. We see that the point $P_0 = (\alpha, 0) \in \mathbb{P}\left(\mathbb{F}_q^2\right)$ with $\alpha^{n/2} = p - 1$ is an $\mathbb{F}_{q^2}-$rational place of the affine curve $y^m = (x^{n/2} + 1)$. The other rational places are $P_k = (\beta, 0)$ with $\beta^{n/2^k} = p - 1, \dots,$ $P_2 = (\beta^2, 0)$, $P_1 = (1, 0)$, $P_0 = (-1, 0)$ and the place $P_\infty = (0, \alpha)$ at ∞. The cyclic code is realised as the algebraic geometric code associated to the divisors $D = P_0 + P_1 + \dots + P_k$, $G = \mu P_\infty$ and the parameter μ satisfies the bound $\mu > 2g - 2$, where g is the genus of the curve $\mathcal{C}_{n,m}$. Note that m is the least integer such that $n | p^m - 1$. In particular α is a generator of $(\mathbb{F}_p)^m$.

If n is an integer odd number, by Theorem 2.3, we know there is a set of roots $\{\alpha^j\}_{j\in J}$, such that α is a generator of $(\mathbb{F}_{p^m})$. Now we consider the points $P_j = (\alpha^j, 0)$ with $j \in J$ and the point P at $P_\infty = (0, \alpha) = \infty$, and the cyclic code is realised as the function field code associated to the divisors $D = \sum_{j\in J} P_j$ and μP_∞. □

Remark 2.6. *The proof given in theorem gives a realisation of cyclic codes as AG codes constructed over the curve with affine model $y^m + x^n = 1$. In particular when $m = n = q + 1$, we cover the codes defined over the Hermitian curve.*

Another important family of cyclic codes is obtained considering the roots of the polynomial $x^n - 1$ over its splitting field. These codes are of great importance in ADN-computing and as they are linear codes, they can be described as function fields. Let α be a primitive element of the underlying vector space over $\mathbb{F}_q$. Since the base field is of characteristic p, $x^n - 1$ has n different zeroes. Let $\overline{\mathbb{F}}_q[x]$ be the extension field containing the n^{th} roots of unity $1, \alpha, \ldots, \alpha^{n-1}$, where $\alpha^{n-1} + \alpha^{n-2} + \ldots + \alpha + 1 = 0$. Moreover the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ constitutes a basis over the prime field $\mathbb{F}_p$, and the field extensions $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(x^{n-1} + \ldots + x + 1)$ are isomorphic.

Example 3. *The polynomial $x^2 + x + 1$ over $\mathbb{F}_p[x]$ is irreducible, thus the fields $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/(x^2 + x + 1)$ are isomorphic, and the roots $w, w + 1$ correspond to one place of degree 2 in the extension field $\mathbb{F}_p(w)$.*

Example 4. *We define the polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, with $a_i \in \mathbb{Q}$, and $f(x, t) = f(x) - t$. Then, if f is a separable polynomial, then the Galois group of $f(x, t)$ over $\mathbb{Q}(t)$ is a regular extension with Galois group S_n.*

Observe that $\mathbb{Q}(x_1 \ldots, x_n)$ is the function field of an $(n-1)-$dimensional projective space $\mathbb{P}^{n-1}(\mathbb{Q})$ over $\mathbb{Q}$. Suppose that $z_1, \ldots, z_n$ are the roots of f in a splitting field of f over $\mathbb{Q}$. Each coefficient a_i of x^i in f is symmetric in $z_1, \ldots, z_n$, thus by the theorem on symmetric functions, we can write a_i as a symmetric polynomial in $z_1, \ldots, z_n$ with rational coefficients. On the other side, for a permutation $\sigma \in S_n$, set $E_\sigma = x_1z_{(\sigma(1))} + \cdots + x_nz_{(\sigma(n))}$ in $\mathbb{Q}(x_1 \ldots, x_n)$ and $f(x) = \prod_\sigma (x - E_\sigma)$, where σ runs through all permutations in S_n.

Theorem 2.7. *(Hilbert) Let $G = S_n$ be acting on $\mathbb{Q}(x_1, \ldots, x_n)$. The field E of S_n-invariants is $\mathbb{Q}(t_1, \ldots, t_n)$, where t_i is the i^{th} symmetric polynomial in $x_1, \ldots, x_n$ and $\mathbb{Q}(x_1, \ldots, x_n)$ has Galois group S_n over E. It is the splitting field of the polynomial $f(x) = x^n - t_1x^{n-1} + \ldots + (-1)^n t_n$.*

Let F be a finite field such that $(char F, n) = 1$. A non-zero polynomial in $\overline{\mathbb{F}}[x, y]$ defines a curve on the plane $\overline{\mathbb{F}}^2$. The elliptic curves are curves of the form $y^2 = f(x)$, where $f(x)$ is a polynomial of degree 3 with coefficients in $\overline{\mathbb{F}}$.

Proposition 2.8. *Let $n = rs$ be a factorisation of an integer positive number n into irreducible coprime factors and assume $r < s$, then there is a sequence of field extensions $\mathbb{F}_{q^r} \subset \mathbb{F}_{q^s} \subset \mathbb{F}_{q^n}$.*

Proof. Consider the map $T_n : F^n \mapsto F^n$

$$t_j = (-1)^j \sigma_j(x_1, \ldots, x_n),$$

where σ_j is the jth elementary symmetric function in the variables x_i. Thus $\{t_j, j = 1, \cdots n\}$, are the coefficients of the equation:

$$f(z, t_1, \ldots, t_n) = z^n + (-1)t_1z^{n-1} + \cdots + (-1)^n t_n = (z - x_1)(z - x_2)\cdots(z - x_n).$$

If we apply Theorem 2.7 to the i^{th} elementary symmetric polynomial in the symbols $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^n}$, we get that the field of S_n invariants of the polynomial

$f(z, t_1, \dots, t_n)$ contains an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. Moreover, for any divisor r of n, one can consider the field of S_r invariants, and apply Theorem 2.7 to the symbols $\alpha, \alpha^{q^{2s}}, \dots, \alpha^{q^{rs}}$, where $n = rs$. Then we get an extension $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^r}$ and all its $\mathbb{F}_q$-subspaces are stable under $Gal\left(\mathbb{F}_{q^s}/\mathbb{F}_{q^r}\right)$. □

Example 5. *Assume $n = q + 1$ and we study again the roots of the polynomial $x^q - 1$ in its splitting field. Let ξ be a non-trivial n-root of unity, for any divisor r of n, one can consider the symbols $\xi^{q^r}, \dots, \xi^q, \xi$. The field of S_r invariants of the polynomial $f(z, t_1, \dots, t_r)$ is the set of solutions to the equation:*

$$x^{q^r} + \dots + x^q + x = a \quad in \quad \mathbb{F}_{q^n}. \tag{2}$$

In $\mathbb{F}_{2^n}$, for any divisor d of n, there are exactly 2^{d-1} solutions to Eq. (2) if n/d is odd and 2^d solutions if n/d is even.

Instead of considering r, s divisors of n, we can consider a partition of n into two parts. For example for an integer $0 \leq k \leq n$, we consider the partition $(k, n-k)$ of n. Fix two elements $g_1, g_2 \in GL(n, q)$ of rank k and rank $n - k$. These points correspond to linear transformations $T_{g_i} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, i \in 1, 2$. It is well known that the corresponding points $\mathbb{F}_{q^k, q^n} \subset \mathbb{F}_{q^n}$ and $\mathbb{F}_{q^{n-k}, q^n} \subset \mathbb{F}_{q^n}$ in the Grassmannians $\mathcal{G}_{k,n}\left(\mathbb{F}_q\right)$ of $k-$dimensional subspaces and the Grassmannian $\mathcal{G}_{n-k}\left(\mathbb{F}_q\right)$ of $n - k$ dimensional subspaces respectively are dual subspaces in the underlying vector space $\left(\mathbb{F}_q\right)^n$ for the Euclidean inner product. Note that the Hamming weight is preserved under invertible linear transformation. This case is of great interest for applications in coding theory, since the corresponding codes with generator matrices G_1 and G_2 respectively are dual codes. Namely, given a linear $[n, k]$-code, a parity check matrix for C is an $(n-k) \times n$ matrix H of rank $n - k$ such that $C = \left\{x \in \left(\mathbb{F}_q\right)^n : Hc^T = 0\right\}$. Then the dual code $C^\perp$ is the linear $[n, n-k]$ code generated by the parity check matrix of C. There is a right action of the general linear group $GL\left(n, \mathbb{F}_q\right)$ on $\mathcal{G}_{k,n}\left(\mathbb{F}_q\right)$:

$$\mathcal{G}_{k,n}\left(\mathbb{F}_q\right) \times GL\left(n, \mathbb{F}_q\right) \to \mathcal{G}_{k,n}\left(\mathbb{F}_q\right) \tag{3}$$

$$(\mathcal{U}, A) \to \mathcal{U}A. \tag{4}$$

One can study the orbits of $\mathcal{G}_{k,n}\left(\mathbb{F}_q\right)$ by the action of any subgroup in the general linear group $GL\left(n, \mathbb{F}_q\right)$. For example we can study the orbit of any triangle group: the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$, the dihedral group, the alternated groups A_4 and A_5 or the symmetric group S_n. Take as T the standard shift operator on $\mathbb{F}_q^n$, a linear code C is said to be quasi-cyclic of index l or $l-$quasi-cyclic if and only if is invariant under T^l. If $l = 1$, it is just a cyclic code. The quantity $m := n/l$ is called the co-index of C. Namely, if we view a codeword $(c_0, c_1, \dots, c_{n-1})$ of C as a polynomial $c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]$, then $T(c(x)) = x \cdot c(x) \mod (x^n - 1)$.

Example 6. *We study the action of a rotation element on the Grassmannian $\mathcal{G}_{2,4}\left(\mathbb{F}_q\right)$ of lines in a 3-dimensional projective space $PG(3, q)$. We apply to any line g a rotation τ of angle $\alpha = \frac{2\pi}{n}$, represented by the array of vectors $<(1, 0, 0), (0, cos\,(\alpha), sin\,(\alpha)), (0, -cos\,(\alpha), sin\,(\alpha))>$. It is easy to see that the orbit code by the composed action τ^m with m divisor of n is a quasi-cyclic code of index $\frac{m}{n}$.*

In general, we study generalised Grassmannians or more commonly known as flag varieties. Fix a partition $\lambda = (\lambda_1, \dots, \lambda_r)$ of n and let $\mathcal{F}_\lambda = \mathcal{F}_\lambda\left(\mathbb{F}_q\right)$ be the variety of partial flags of $\mathbb{F}_q-$vector spaces

$$\{0\} = E^r \subset E^{r-1} \subset \ldots \subset E^1 \subset E^0 = \left(\mathbb{F}_q\right)^n$$

such that $\dim\left(E^{i-1}/E^i\right) = \lambda_i$. The group $GL\left(n, \mathbb{F}_q\right)$ acts on $\mathcal{F}_\lambda$ in the natural way. Fix an element $X_0 \in \mathcal{F}_\lambda$ and denote by $\mathcal{P}_\lambda$ the stabilizer of X_0 in G and by $\mathcal{U}_\lambda$ the subgroup of elements $g \in \mathcal{P}_\lambda$ which induces the identity on E^i/E^{i+1} for all $i = 0, 1, \ldots, n-1$. Put $\mathcal{L}_\lambda = GL_{\lambda_r}\left(\mathbb{F}_q\right) \times \ldots, \times GL_{\lambda_1}\left(\mathbb{F}_q\right)$, then we have $\mathcal{P}_\lambda = \mathcal{L}_\lambda \times \mathcal{U}_\lambda$.

Proposition 2.9. *Let us consider the factorisation of n into irreducible pairwise coprime factors* $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ *with* $e_1 < e_2 < \ldots < e_r$, *and* $\lambda = (e_1, \ldots, e_r)$ *be the partition of exponents. Then there is a flag variety* $\mathcal{F}_\lambda\left(\mathbb{F}_q\right)$ *of partial flags of* $\mathbb{F}_q$*−vector spaces:*

$$\{0\} = E^r \subset E^{r-1} \subset \cdots \subset E^1 \subset E^0 = \left(\mathbb{F}_q\right)^n,$$

such that $dim\left(E^{i-1}/E^i\right) = e^i$.

Proof Observe that the result follows trivially for the case in which n is a prime number $e_1 = \cdots = e_r = 1$. If $n = rs$ factorizes into two irreducible prime factors, the result follow as we have seen above, there is a flag $\{0\} = E^r \subset E^s \subset E^0 = \left(\mathbb{F}_q\right)^n$ and then by induction in r the result follows. □

Given a cyclic code over $\overline{F}$ of length n, its defining set is given by the exponents occurring in $g(x)$, where $g(x)$ is the generator polynomial of the ideal of the code in $F[x]/(x^n - 1)$.

Let $\alpha \in \overline{F}$ be an n^{th} primitive root of unity. The n^{th} cyclotomic polynomial $\Phi_n(x) = \prod_{1<j<n,(j,n)=1}\left(x - \alpha^j\right) \in \overline{F}[x]$ is the minimal polynomial of α over F. It is monic of degree of the Euler's totient function $\varphi(n)$. It has integer coefficients and it is irreducible over $\mathbb{Q}$. In $\mathbb{Q}[x]$, we have the factorization into irreducible polynomials:

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

By Möebius inversion:

$$\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)}$$

In the case of binary codes where $q = 2$, Bezzateev and Shekhunova [8] have obtained that the number of irreducible normalized polynomials $I_{2^m}(l)$ of degree l over $\mathbb{F}_{2^m}$ satisfy the following equation:

$$I_{2^m}(l) = \frac{1}{l} \sum_{d/l} \mu(d) 2^{m\frac{l}{d}}. \tag{5}$$

where $\mu(d)$ is the Möebius function:

$$\mu(d) = \begin{cases} 1 \ \ if \ \ d = 1; \\ (-1)^r \ \ if \ \ d \ \ is \ \ a \ \ product \ \ of \ \ r \ \ different \ \ prime \ \ numbers; \\ 0 \ \ in \ \ all \ \ other \ \ cases. \end{cases}$$

Let $g(x)$ equals the least common multiple $lcm\left\{\Phi_i(x) : \alpha^i \in S\right\}$, then S is a defining set for C. We will describe the defining set by the exponents occurring in S with $S = \{i_1, i_2, \ldots, i_l\}$, where $i_1 < \ldots < i_l$. A parity check matrix for the code $C(S)$ is given by:

$$M(S) = \begin{pmatrix} \left(\alpha^{i_1}\right)^0 & \left(\alpha^{i_1}\right)^1 & \cdots & \left(\alpha^{i_1}\right)^{n-1} \\ \left(\alpha^{i_2}\right)^0 & \left(\alpha^{i_2}\right)^1 & \cdots & \left(\alpha^{i_2}\right)^{n-1} \\ \vdots & & \vdots & \\ \left(\alpha^{i_r}\right)^0 & \left(\alpha^{i_r}\right)^1 & \cdots & \left(\alpha^{i_r}\right)^{n-1}) \end{pmatrix}$$

The code $C \subset F^n$ is obtained as the subfield subcode of $\overline{C}$:

$$C = \left\{c \in F^n : M(R)c^T = 0\right\}.$$

Given a triple (I, J, K) of subsets of $\{1, \dots, n\}$ of the same cardinality r, we associate to them partitions λ, μ and ν as follows. Let $I = \{i_1 < \dots < i_r\} \subset \{1, \dots, n\}$, then the corresponding partition is defined as $\lambda = (i_r - r, \dots, r_1 - 1)$, and respectively for J, K. We call the triple (I, J, K) admissible for the Horn problem, if the corresponding triple of partitions (λ, μ, γ) occurs as eigenvalues of a triple of Hermitian r by r matrices, with the third one the sum of the first two.

We describe Horn's inductive procedure to produce set of triples $(I, J, K) \subset \{0, 1, \dots, n\}$.

$$U_r^n = \left\{(I, J, K) | \sum_{i \in I} i + \sum_{j \in J} j = \sum_{k \in K} k + r(r+1)/2\right\},$$

$$T_r^n = \{(I, J, K) \in U_r^n | \ for \ \ all \ \ p < r \ \ and \ \ all \ \ (F, G, H) \in T_p^r,$$

$$\sum_{f \in F} i_f + \sum_{g \in G} j_g \leq \sum_{h \in H} k_h + p(p+1)/2\}.$$

Example 7. *Let us consider the triple of subsets*

$$(I, J, K) = (\{1, 3, 5\}, \{1, 3, 5\}, \{2, 4, 6\})$$

and the corresponding triple of partitions $(\lambda, \mu, \nu) = ((2, 1, 0), (2, 1, 0)(3, 2, 1))$ arises from the triple of diagonal 3 by 3 matrices with diagonal entries $(2, 1, 0), (1, 0, 2)$ and $(3, 1, 2)$.

Lemma 2.10. *For any triple (I, J, K) admissible for the Horn problem, the polynomials defined by $f(x) = \prod_{i \in I}(x - \alpha^i), g(x) = \prod_{j \in J}(x - \alpha^j)$, and $h(x) = \prod_{k \in K}(x - \alpha^k)$ generate a cyclic code of length $n = i_r + j_r + k_r mod p$ and $k = r$, where $r = \ |I| + |J| + |K|$ and p is the characteristic of the field F.*

Proof. The cyclic code generated by $f(x)$ coincides with the cyclic code generated by $lcm\{m_i(x) : \alpha^i, i \in I\}$ and respectively for $g(x)$ and $h(x)$ the polynomials $lcm\{m_j(x) : \alpha^j, j \in J\}$ and $lcm\{m_k(x) : \alpha^k, k \in K\}$. It is the cyclic code generated by the minimal polynomial of $\alpha^{i_r + j_r + k_r}$. □

Remark 2.11. *We see that Horn's algorithm is relevant since some classical code constructions can be seen as ideals in a finite dimensional commutative semi simple algebra over a finite field $\mathbb{F}_q$ with $q = p^r$ elements and p a prime number as in example (3).*

Lemma 2.12. *The family of cyclic codes obtained by considering the roots of the polynomial $x^n - 1$ over its splitting fields are indeed AG codes arising from genus 0 curves, and by Riemann-Roch theorem, their parameters satisfy the bound $d \geq n + 1 - k$, where d is the minimum distance.*

Proof Let $\overline{\mathbb{F}}_q[x]$ be the extension field containing the n^{th} roots of unity $1, \alpha, \dots, \alpha^{n-1}$, where $\alpha^{n-1} + \alpha^{n-2} + \dots + \alpha + 1 = 0$. Moreover the set $\left\{1, \alpha, \dots, \alpha^{n-1}\right\}$

constitutes a basis over the prime field $\mathbb{F}_p$, and the field extensions $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(x^{n-1} + \ldots + x + 1)$ are isomorphic. □

2.3 Generating functions of conjugacy classes in a group

The automorphism group of the projective line $\mathbb{P}(\mathbb{F}_q)$ is the projective linear group $PGL(2, q)$. Any finite subgroup $A \subset PGL(2, q)$ defines a $k-$uniform Cayley (sum) hypergraph $\Gamma^k(A)$ whose vertices are the generating $k-$tuples of A and the edges are $k-$element sets $\{x_1, \ldots, x_k\} \in \binom{G}{k}$ represented by random variables $x_1, \ldots, x_k$. In particular, if $f(z)$ is the ordinary generating function that enumerates A, that is, number of conjugacy classes in A, then $\frac{1}{1-f(z)}$ is the ordinary generating function enumerating sequences of k elements in A. If G is an abelian group, then $x_1 + \cdots + x_k \in A$. In general, we will consider k-arcs in $\Gamma(A)$ which represent casual connections between the variables. Applications are known in statistics, for example the multinomial experiment consists of n identical independent trials, and there are k possible outcomes (classes, categories or cells) to each trial and the cell counts $n_1, n_2, \ldots, n_k$ are the random variables, the number of observations that fall into each of the $k-$categories.

Definition 2.13. *In $PG(n-1, q)$ a $(k; r)-$arc is a set of k points any r of which form a basis for $\mathbb{F}_q^n$, or in other words, $r-1$ of them but not r are collinear.*

Consider the normal rational curve over $\mathbb{F}_q$:

$$\mathcal{V}_1^n := \{\mathbb{F}_q(1, x, x^2, \ldots, x^n) \mid x \in \mathbb{F}_q \cup \{\infty\}\}$$

is a $(q + 1)$-arc in the n-dimensional projective space $PG(n, q)$.

We see that if $q \leq n$, the NRC is a basis of a q-dimensional projective subspace, that is, a $PG^q(n, q)$. So we can enumerate how many NRC's are there in a $PG(n, q)$. The answer is $\phi(q; n, q)$, the number of ways of choosing such a set of points in a particular q-space. If $q \geq n + 2$, the NRC is an example of a $(q + 1)$-arc. It contains $q + 1$ points, and every set of $n + 1$ points are linearly independent.

2.4 Conclusion

The problem of considering finite subgroups and conjugacy classes in $PGL(2, q)$ the automorphism group of the projective line can be generalised to that of finite subgroups in $PGL(n, q)$, the collineation group of the normal rational curve.

Acknowledgements

This research has been partially supported by the COST Action IC1104 and the project ARES (Team for Advanced Research on Information Security and Privacy. Funded by Ministry of Economy and Competitivity).

Author details

Cristina Martinez Ramirez* and Alberto Besana
Department of Maths, UAB, Barcelona

*Address all correspondence to: cristinamartine@gmail.com

References

[1] Kötter R, Kschischang FR. Coding for errors and erasures in random network coding. IEEE Transactions on Information Theory. 2008;**54**(8)

[2] Garcia A, Stichtenoth H. On the asymptotic behaviour of some towers of function fields over finite fields. Journal of Number Theory. 1996;**61**(2):248-273

[3] Geil O, Martin S, Martínez-Peas U, Ruano D. Refined analysis of RGHWs of code pairs coming from Garcia-Stichtenoth's second tower. In: Proceedings of 21st Conference on Applications of Computer Algebra

[4] Bezzateev SV, Shekhunova NA. Subclass of cyclic Goppa codes. IEEE Transactions on Information Theory. Nov. 2013;**59**(11)

[5] Niederreiter H, Xing C, Lam KY. A new construction of algebraic-geometry codes. Applicable Algebra in Engineering, Communication and Computing. 1999;**9**:373-381

[6] Hachenberger D, Niederreiter H, Xing C. Function field codes. Applicable Algebra in Engineering, Communication and Computing. 2008;**19**:201-211

[7] Couvreur A, Márquez I, Pellikaan R. A polynomial time attack against algebraic geometry code based public key cryptosystems. arXiv:1401.6025

[8] Bezzateev SV, Shekhunova N. Class of generalized Goppa codes perfect in weighted hamming metric. Des. Codes Criptogr. 2013;**66**:391-399